РЕПУБЛИКА БЪЛГАРИЯ
ОБЛАСТЕН УПРАВИТЕЛ НА ОБЛАСТ ВАРНА

ЗАПОВЕД

№ РД-21-7711-9

21.10. 2021г

МАРИО СМЪРКОВ – областен управител на област с административен център град Варна

У С Т А Н О В И Х:

Със заповед № РД-18-7711-6/28.05.2018г на областния управител на област Варна са одобрени „Вътрешни правила за обработване и защита на личните данни на физически лица в Областна администрация Варна" (за краткост ще бъдат наричани само Вътрешни правила нататък в заповедта), свързани с прилагането на Общ регламент за защита на личните данни 2016/679 на Европейския съюз.

Защитата на правата на физическите лица във връзка с обработването на лични данни изисква приемане на подходящи технически и организационни мерки, за да се гарантира изпълнението на изискванията на посочения регламент. Същият предоставя възможност на различните засегнати от разпоредбите му органи да приложат изискванията чрез адаптиране към спецификите в тяхната дейност и функции. За да може да докаже съответствието с настоящия регламент, администраторът следва да приеме вътрешни правила и да приложи мерки, които отговарят на принципите за защита на личните данни, заложени в европейското и националното законодателство.

Съгласно нормативните изисквания публичните органи, в качеството си на администратори на лични данни, следва да определят длъжностно лице по защита на данните. С цел оптимизиране на взаимодействието между звената в Областна администрация Варна при събиране, използване, съхранение и защита на лични данни на физически лица, както и предвид преобладаващия електронен характер на посочените процеси, Вътрешните правила следва да бъдат актуализирани.

С оглед на гореизложеното и на основание чл. 32, ал. 1 от ЗА

Н А Р Е Ж Д А М:

Изменям действащите „Вътрешни правила за обработване и защита на личните данни на физически лица в Областна администрация Варна" по следния начин:

1. ***Чл. 33*** от действащите Вътрешни правила се изменя и се чете:

(1) Длъжностното лице по защита на личните данни е служител в Областна администрация Варна, определен със заповед на областния управител, на когото не е изрично възложено да предоставя информация, с цел предотвратяване конфликт на интереси. В качеството си на лице по защита на личните данни, служителят се отчита директно пред областния управител, на когото при необходимост дава препоръки или съобщава за рискове, свързани с администрирането на лични данни.

(2) Задълженията на служителя в областта на защитата на лични данни се вписват в длъжностната му характеристика.

2. ***Чл. 35*** от действащите Вътрешни правила се отменя изцяло.

3. ***Чл. 37*** от действащите Вътрешни правила се изменя и се чете:

(1) При определяне на длъжностното лице по защита на личните данни се отчитат следните критерии и изисквания, изведени от контекста на Регламент (ЕС) 2016/679 и

РЕПУБЛИКА БЪЛГАРИЯ

ОБЛАСТЕН УПРАВИТЕЛ НА ОБЛАСТ ВАРНА

УТВЪРЖДАВАМ:

ОБЛАСТЕН УПРАВИТЕЛ: / П /

/СТОЯН ПАСЕВ/

ВЪТРЕШНИ ПРАВИЛА

ЗА ОБРАБОТВАНЕ И ЗАЩИТА НА ЛИЧНИТЕ ДАННИ НА ФИЗИЧЕСКИ ЛИЦА В ОБЛАСТНА АДМИНИСТРАЦИЯ ВАРНА

2018г

съхраняването и използването на документите в учрежденския архив на Областна администрация Варна, утвърдени от областния управител и началникът на отдел „Държавен архив" Варна.

(2) Относно сроковете за съхраняване и унищожаването на данни на хартиен носител се отчитат и становищата на постоянно действаща експертна комисия по организиране на архивния фонд към Областна администрация Варна.

(3) С цел да се гарантира, че срокът на съхранение на личните данни не е по-дълъг от необходимия, администраторът установява срокове, приложени към Вътрешни правила за използване и съхранение на документи в архива на Областна администрация Варна, за унищожаване на преписки на хартиен носител и изтриване на сканираните им копия от електронната деловодна система на ведомството. При фиксирането на тези срокове се отчита становището на представител на „Държавен архив" дали определени документи не следва да бъдат предадени за съхрание в Националния архивен фонд.

Чл.8. (1) Администраторът следва да осигури на субектите възможност да коригират или заличават неточните лични данни.

(2) Личните данни следва да се използват и съхраняват по начин, гарантиращ подходяща степен на сигурност и поверителност, включително за предотвратяване на непозволен достъп до тях и до оборудване за обработването им.

(3) Администраторът не следва да запазва лични данни с единствената цел да може да реагира на евентуални искания.

Чл.9. (1) Настоящите правила се прилагат за обработването на лични данни на физически лица изцяло или частично с автоматични средства, както и за обработването с други средства на такива данни, които са или предназначени да бъдат част от регистър с персонални данни.

(2) Правилата не обхващат обработването на лични данни, които засягат юридически лица.

(3) Правилата не се отнасят за лични данни на починали лица, към които се прилагат общите правила за документооборот в Областна администрация Варна.

Чл.10. Общият регламент за защита на личните данни 2016/679 на Европейския съюз въвежда легални дефиниции, с които публичният администратор на лични данни следва да съобразява дейността си. Предвди това за нуждите на документооборота в Областна администрация Варна и защитата на съдържащите се в него лични данни на физически лица, в работните стандарти на ведомството се интегрират следните понятия:

а) „лични данни" представляват всяка информация, свързана с идентифицирано физическо лице или такова, чиято легитимация може да бъде установена въз основа на тези данни - субект на данни;

б) „обработване" означава всяка операция или съвкупност от операции, извършвана с лични данни чрез автоматични или други средства като събиране, записване, организиране, структуриране, съхранение, адаптиране или промяна, извличане, консултиране, употреба, разкриване чрез предаване, разпространяване или друг начин, по който данните стават достъпни, подреждане или комбиниране, ограничаване, изтриване или унищожаване;

в) „ограничаване на обработването" означава маркиране на съхранявани лични данни с цел ограничаване на обработването им в бъдеще;

г) „псевдонимизация" означава обработването на лични данни по такъв начин, че личните данни не могат повече да бъдат свързвани с конкретен субект на данни, без да се използва допълнителна информация, при условие че тя се съхранява отделно и е предмет на технически и организационни мерки с цел да се гарантира, че личните данни не са свързани с идентифицирания им субект;

д) „регистър с лични данни" означава всеки структуриран набор от лични данни, достъпът до които се осъществява съгласно определени критерии;

ПРИНЦИПИ ПРИ ОБРАБОТВАНЕТО НА ЛИЧНИ ДАННИ

Чл.13. (1) Личните данни се обработват законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните.

(2) Данните се събират за конкретни, изрично указани, легитимни и ясно дефинирани цели и не се обработват по-нататък по начин, несъвместим с тези цели; по-нататъшното обработване за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели не се счита за несъвместимо с първоначалните цели.

(3) Събират се подходящи данни, ограничени до необходимото и свързани с целите, за които се обработват.

(4) Следва да се събират актуални данни и да се предприемат разумни мерки, за да се гарантира своевременното изтриване или коригиране на неточни лични данни, като се имат предвид целите, за които те се обработват.

(5) Личните данни се съхраняват във форма, която да позволява идентифицирането на субекта им за период, не по-дълъг от необходимото за целите, за които се обработват; личните данни могат да се съхраняват за по-дълги срокове, доколкото ще бъдат обработвани единствено за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели, както и в съответствие с предвидените в нормите за Националния архивен фонд срокове; следва да бъдат приложени подходящите технически и организационни мерки с цел да бъдат гарантирани правата и свободите на субекта на данните.

(6) Данните се обработват по начин, гарантиращ подходящо ниво на сигурност и поверителност, включително защита срещу неразрешено или незаконосъобразно обработване и случайна загуба, унищожаване или повреждане, като се прилагат подходящи технически и организационни мерки.

Чл.14. (1) Личните данни са обикновени и специални.

а) обикновените се делят на:

- свързани с физическата идентичност на лицата – три имена, постоянен и настоящ адрес, ЕГН, номер на личната карта, орган и дата на издаването й, електронен адрес, телефон;
- свързани с икономическата идентичност – имотно и финансово състояние, участие и/или притежание на дялове, ценни книжа в дружества, наличие на публични задължения, данни, необходими за идентифициране за целите на данъчното законодателство, данъчен идентификационен номер;
- свързани със социалната идентичност – образование, трудова дейност, гражданство;
- свързани със семейната идентичност - семейно положение, родствени връзки.

б) специалните лични данни се наричат още „чувствителни" и разкриват расов или етнически произход, политически възгледи, религиозни или философски убеждения, членство в синдикални организации, генетични данни, биометрични данни, данни за здравословното състояние, данни за сексуалния живот или сексуалната ориентация на физическото лице.

(2) Обработването на специални лични данни се забранява, освен ако:

а) субектът на данни е дал своето изрично съгласие за обработването им за една или повече конкретни цели, освен когато в националното или европейско право се предвижда, че забраната не може да бъде отменена от субекта на данни;

б) обработването е необходимо за изпълнение на задълженията или упражняването на специални правомощия на администратора или за осъществяване на права на субекта на данните по силата на действаща нормативна хипотеза;

в) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;

г) обработването е свързано с лични данни, които явно са направени обществено достояние от субекта на данните;

(4) Администраторът запознава всичките си служители с основните изисквания на Регламент за защита на личните данни 2016/679, което се удостоверява с подписа им в Регистър за информираност на служителите относно правилата за работа с лични данни на физически лица (Приложение № 3), който се съхранява при експерт „Човешки ресурси".

(5) Лични данни на физически лица се съхраняват в преписките на хартиен носител, в електронната деловодна система на ведомството и в лично създадените файлове от всеки служител. Служителят взема необходимите мерки да спазва правилата за правомерно обработване на лични данни на физически лица, съобразно целите на обработката. Непотребни документи, съдържащи лични данни, се изхвърлят от ведомството след механично унищожаване на носителя им.

(6) Администраторът прилага политика на „чистото бюро", която всички служители, обработващи лични данни, прилагат. Записите върху хартиен носител не трябва да се оставят там, където могат да бъдат достъпни за неоторизирани лица и не бива да бъдат изваждани от помещенията на администратора без изрично разрешение или конкретна процесуална нужда, присъща за функциите на администрацията. Веднага щом хартиените документи вече не са необходими за текущата работа по обработване на лични данни, те следва да бъдат архивирани по съответния ред, а ако липсва основание за тяхното архивиране, следва да бъдат унищожени в съответствие със създадена за това процедура.

Чл.17. (1) В случай, че администраторът обработва лични данни на основание единствено съгласието на лицето, законосъобразността на действията му се потвърждава, когато администраторът докаже, че:

а) съгласието е свободно изразено и е не е дадено под натиск или заплаха от неблагоприятни последици;

б) съгласието е конкретно – за всяка определена цел, а когато е относимо - и за отделна категория лични данни;

в) съгласието е информирано – дадено въз основа на пълна, точна и лесно разбираема информация;

г) съгласието е недвусмислено – не се предполага, а е израз на пряко волеизявление или ясно потвърждаващо действие; мълчанието или липсата на волеизявление в тази насока не може да се приеме за съгласие.

(2) Съгласието по ал. 1 се документира в декларация, неразделна част от настоящите правила (Приложение 1).

(3) Ако физическото лицето откаже да подпише декларация за информирано съгласие, се съставя протокол, подписан от служителя „Административно обслужване" и длъжностното лице по защита на личните данни или юрисконсулт от ведомството, с който се удостоверява направения отказ, въпреки предоставената от администратора информация.

(4) На субекта на данните се предоставя възможност по всяко време да оттегли съгласието си с процедура аналогична на тази, с която го е дал.

Чл.18. (1) Съгласие следва да се дава чрез ясен утвърдителен акт – действие, което категорично показва, че субектът на данни е съгласен с предложеното обработване на неговите лични данни. Поради това мълчанието, предварително отметнати полета на хартиен или технически носител или липсата на действие не представляват съгласие.

(2) Съгласието следва да обхваща всички дейности по обработване, извършени за една и съща цел или цели. Когато обработването преследва повече цели, за всички тях следва да бъде дадено съгласие.

(3) Когато обработването се извършва въз основа на съгласието на субекта на данните, администраторът следва да може да докаже, че субектът на данните е дал съгласието си за операцията по обработване. Администраторът осигурява предварително съставена декларация за съгласие в разбираема и лесно достъпна форма, която не съдържа неравноправни клаузи.

(4) За да бъде съгласието информирано, субектът на данни следва да знае самоличността на администратора и целите на обработването, за които са предназначени личните данни.

д) право на преносимост на данните – ако се обработват по автоматизиран начин на основание съгласие или договор; за целта данните се предават в структуриран, широко използван и пригоден за машинно четене формат; ако е технически осъществимо, прехвърлянето на данните може да стане пряко от един администратор към друг при спазване на процедурите, свързани с комплексното административно обслужване; правото на преносимост обхваща само данни, предоставени лично от субекта им, както и лични данни, генерирани и събрани от неговата дейност;

е) право на възражение, което може да се упражни по всяко време и на основания, свързани с конкретна претенция на лицето, при условие, че не съществуват убедителни законови основания за обработването, които да са с предимство пред интересите, правата и свободите на субекта на данните или го засягат в значителна степен;

ж) субектът на данни има право да не бъде обект на изцяло автоматизирано решение, включващо профилиране, което поражда правни последици за субекта на данните или го засяга в значителна степен.

(2) В случай, че администраторът разполага с лични данни на лице, което не му ги е предоставило само, при поискване следва да разкрие на лицето източника на личните данни и дали той е публично достъпен.

(3) Администраторът не е задължен да удовлетворява искания за изтриване на лични данни от физически лица, ако са налице нормативни предпоставки за съхранението или обработката им. Администраторът обаче е длъжен да документира подобно искане в определен за целта регистър, както и своя отговор по него.

(4) Когато лични данни са станали достояние на администратора нецеленасочено, като косвен резултат от изпълнението на негово законово правомощие или задължение (видеозапис на лице, преминало през зоната за охранително видеонаблюдение) администраторът не е длъжен да предостави достъп до тази информация на лицето повече от веднъж.

(5) Когато исканията на субект на данни са явно неоснователни или прекомерни, по-специално поради своята повторяемост, администраторът може да наложи разумна такса, като взема предвид административните разходи за предоставяне на информацията или извършването на исканите действия, или да откаже да предприеме действия по искането. В тези случаи администраторът носи тежестта на доказване на явно неоснователния или прекомерен характер на искането.

Чл.20. (1) Правото на субекта на данни да предава или получава отнасящи се до него лични данни не поражда задължение за администраторите да придобиват или поддържат технически съвместими системи за обработване. Когато в определен пакет от лични данни е засегнат повече от един субект на данни, правото личните данни да бъдат получавани следва да не засяга правата и свободите на други субекти на данни.

(2) Когато това е технически осъществимо, субектът на данни има право на пряко прехвърляне на личните данни от един администратор към друг.

Чл.21. Дори когато личните данни се обработват законно - обработването е необходимо за изпълнението на задача от обществен интерес, при упражняването на официално правомощие, предоставено на администратора, или по съображения, свързани със законните интереси на администратора или трета страна - всеки субект на данни има право на възражение срещу обработването на лични данни, свързани с неговото конкретно положение. Администраторът следва да докаже, че неговите неоспорими законни интереси имат преимущество пред интересите или основните права на субекта на данни.

Чл.22. (1) Без да се засягат които и да било други административни или съдебни средства за правна защита, всеки субект на данни има право да подаде жалба до надзорния орган – Комисия за защита на личните данни (КЗЛД), ако счита, че обработването на лични данни, отнасящи се до него, нарушава относимите правни разпоредби. Надзорният орган, до

данните до минимум и интегриране на необходимите гаранции в процеса на обработване чрез специализиран софтуер.

(3) Предприемат се на мерки по подразбиране, които да гарантират, че без намеса на физическото лице личните му данни няма да са достъпни за неограничен брой потребители. Въвеждат се подходящи технически мерки, за да се гарантира, че се обработват само лични данни, които са необходими с конкретна цел.

Чл.28. Прилагането на псевдонимизация на личните данни служи да намали рисковете за съответните субекти на данни и да помогне на администратора и обработващия лични данни да изпълняват своите задължения за защита на данните.

Чл.29. (1) Експерт „Човешки ресурси" от структурата на администратора, в сътрудничество с длъжностното лице по защита на личните данни, следва да приведе досиетата на служителите и работниците във ведомството в съответствие с изискванията на Регламент 2016/679 (ЕС). Медицински изследвания, освен медицинското свидетелство при постъпване на работа и решения от органите на медицинска експертиза (ТЕЛК), както и копия на лични карти не се изискват за досиетата на заетите в държавната администрация.

(2) Експерт „Човешки ресурси" от структурата на администратора следи автобиографиите на кандидати за работа да бъдат използвани еднократно в рамките на конкурса за длъжността, за която са подадени. Без съгласието на отпадналите кандидати документите им не следва да се използват за контакт с тях в последващ момент, при възникване на необходимост за администратора и показани добри резултати в конкурса.

(3) При постъпване на нови служители в Областна администрация Варна към първоначалния комплект с документи експерт „Човешки ресурси" връчва и декларация за поверителност (Приложение № 2), в която е изложено каква информация се събира за лицето и как се използва, както и каква отговорност носи служителят по отношение на работата си с лични данни на други лица.

ДЛЪЖНОСТНО ЛИЦЕ ПО ЗАЩИТА НА ДАННИТЕ

Чл.30. Публичните органи като администратори на лични данни определят длъжностно лице по защита на данните, което има за основна задача да информира и съветва администратора и неговите служители по всички въпроси, свързани с обработването и защитата на личните данни.

Чл.31. Длъжностното лице по защита на данните има ключова роля за осигуряване на законосъобразното обработване на лични данни в структурата на администратора. То следва да разполага с експертни познания в областта на относимото законодателство и/или информационните технологии.

Чл.32. Длъжностното лице по защита на данните не определя целите и средсдтвата за обработване на данни и администраторът не може да му прехвърля своята отговорност за неспазване на нормативните изисквания в тази сфера.

Чл.33. *(изм. със заповед № РД-21-7711-9/21.10.2021г на областния управител на област Варна)*

(1) Длъжностното лице по защита на личните данни е служител в Областна администрация Варна, определен със заповед на областния управител, на когото не е изрично възложено да предоставя информация, с цел предотвратяване конфликт на интереси. В качеството си на лице по защита на личните данни, служителят се отчита директно пред областния управител, на когото при необходимост дава препоръки или съобщава за рискове, свързани с администрирането на лични данни.

(2) Задълженията на служителя в областта на защитата на лични данни се вписват в длъжностната му характеристика.

Чл.39. Отчетността е задължение на администратора на лични данни и основен инструмент за доказване изпълнението на релевантните правни изисквания. Отчетност е способността във всеки един момент администраторът на лични данни да удостовери и докаже, че обработва личните данни добросъвестно, законосъобразно и прозрачно, за адекватни и пропорционални цели, с подходящо ниво на сигурност и защита.

Чл.40. Основните средства за спазване на принципа на отчетност са:

- поддържането на регистри на дейностите по обработване;
- определяне на длъжностно лице по защита на личните данни;
- извършване на оценка на въздействието при наличие на висок риск за правата и свободите на физическите лица;
- своевременно уведомяване на Комисията за защита на личните данни и субекта на данните при нарушения на сигурността;
- полагане на усилия за минимизиране на вредите за засегнатото лице при наличие на пробив в сигурността за съхраняваните лични данни.

Чл.41. (1) Всеки администратор или негов упълномощен представител поддържа регистър на дейностите по обработване, за които отговоря. Този регистър съдържа:

а) името и координатите за връзка на администратора, а когато е приложимо - на всички съвместни администратори, на представителя на администратора и на длъжностното лице по защита на данните;

б) целите на обработването;

в) описание на категориите субекти на данни и на категориите лични данни;

г) категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получателите в трети държави или международни организации;

д) когато е приложимо, предаването на лични данни на трета държава или международна организация;

е) когато е възможно, предвидените срокове за изтриване на различните категории данни;

ж) общо описание на техническите и организационни мерки за сигурност.

(2) Регистрите се поддържат основно в електронен формат, осигуряващ възможност за обективиране на хартиен носител при нужда. При поискване администраторът или обработващият лични данни осигуряват достъп до регистъра на надзорния орган.

(3) Към регистрите не се прикачват лични данни.

Чл.42. (1) Публични органи, пред които се разкриват лични данни в съответствие с правно задължение за упражняване на официалната им функция, например данъчни и митнически органи, звена за финансово разследване или независими административни органи, не следва да се разглеждат като получатели, ако получават лични данни, които са необходими за провеждането на конкретно разследване от общ интерес, в съответствие с националното право или това на Европейския съюз.

(2) Исканията за разкриване на данни, изпратени от публичните органи, следва винаги да бъдат в писмена форма, да са обосновани и да засягат само отделни случаи, като не следва да се отнасят до целия регистър с лични данни или да водят до свързване на регистри на лични данни. Обработването на личните данни от посочените публични органи следва да е в съответствие с приложимите правила за защита на данните съобразно целите на обработването.

Чл. 43. (1) С цел да се поддържа сигурността и да се предотврати обработване, което е в нарушение на принципите за работа с лични данни, администраторът или обработващият следва да извърши оценка на рисковете, свързани с обработването, и да предприеме мерки за ограничаване на тези рискове, например криптиране. Тези мерки следва да гарантират подходящо ниво на сигурност, включително поверителност, като се вземат предвид

- цели на обработването;

- описание на категориите субекти на данни и категориите лични данни;

- категориите получатели, пред които са или ще бъдат разкрити личните данни, включително получатели в трети държави или международни организации;

- предвидените срокове за изтриване на различните категории данни;

- общо описание на техническите и организационни мерки за сигурност.

(3) Информацията по ал. 2 се публикува на интернет страницата на Областна администрация Варна в раздела, обособен за субектите на данни по чл. 16 от настоящите Правила.

Чл.49. (1) Надзорен орган по въпросите за защита на личните данни на физически лица е Комисия за защита на личните данни. Тя има следните основни функции и правомощия:

а) наблюдава и осигурява прилагането на нормативните изисквания;

б) дава становища, в съответствие с действащите правни норми, отнсно законодателните и административните мерки, свързани със защитата на правата и свободите на физическите лица по отношение на обработването;

в) насърчава информираността на администраторите и обработващите лични данни за задълженията им по силата на нормативната уредба;

г) при поискване предоставя информация на всеки субект на данни във връзка с упражняването на правата му по силата на правилата за работа с лични данни;

д) разглежда жалбите, подадени от субект на данни или от структура, организация или сдружение и разследва предмета на жалбата, доколкото това е целесъобразно;

е) дава становища по операциите за обработване на данни;

ж) разпорежда на администратора и на обработващия лични данни да предоставят всяка информация за изпълнението на своите задачи;

з) провежда разследвания под формата на одити във връзка със защитата на данните;

и) уведомява администратора или обработващия лични данни за предполагаемо нарушение на нормативните правила;

й) получава от администратора и обработващия лични данни достъп до всички лични данни и до цялата информация, от която се нуждае за изпълнението на своите задачи;

к) получава достъп до всички помещения на администратора и обработващия лични данни, включително до всяко оборудване и средство за обработване на данни;

л) отправя предупреждения до администратора или обработващия лични данни, когато има вероятност операции по обработване на данни, които те възнамеряват да извършат, да нарушат законовите разпоредби;

м) отправя официално предупреждение до администратора или обработващия лични данни, когато операции по обработване на данни са нарушили правните разпоредби;

н) разпорежда на администратора или обработващия лични данни да изпълнят исканията на субекта на данни да упражнява правата си съгласно действащите правни норми;

о) налага временно или окончателно ограничаване, в това число и забрана за обработването на данни;

п) разпорежда коригирането или изтриването на лични данни или ограничаването на обработването им;

р) налага административно наказание „глоба“ или „имуществена санкция“ в допълнение към другите санкции или вместо тях, в зависимост от особеностите на всеки отделен случай;

с) разпорежда преустановяването на потока на данни към получател в трета държава или към международна организация;

т) одобрява задължителните вътрешни правила на администраторите или обработващите данни.

(2) Надзорният орган има правомощието да дава разрешения и становища:

а) на администратора в съответствие с процедурата по предварителна консултация;

Чл.54. (1) Администраторът или обработващ личните данни следва да прилага псевдонимизация и криптиране на личните данни, както и да проявява устойчива способност за гарантиране на постоянна поверителност, цялостност, наличност и устойчивост на системите и услугите за обработване.

(2) Администраторът или обработващ личните данни осигурява своевременно възстановяване на наличността и достъпа до личните данни в случай на инцидент и осъществява преценка на ефективността на техническите и организационни мерки с оглед гарантиране сигурността на обработването.

Чл.55. Законен интерес на съответния администратор на данни представлява обработването на лични данни в степен строго необходима и пропорционална на целите за гарантиране на мрежовата и информационна сигурност - способността на дадена мрежа или информационна система да издържа, със съответно равнище на доверие, на случайни събития или неправомерни или злонамерени действия, които повлияват на наличността, автентичността, целостта и поверителността на съхраняваните или предавани лични данни, както и на сигурността на свързаните услуги, предлагани или достъпни посредством тези мрежи и системи от страна на публичния орган.

Чл.56. Администраторът следва да използва всички разумни мерки за проверка на самоличността на субекта на данни, който иска достъп, по-специално по отношение на онлайн услугите и онлайн идентификаторите.

Чл.57. В автоматизираните регистри на лични данни ограничаването на обработването следва да бъде осигурено с технически средства, така че личните данни да не подлежат на операции за по-нататъшно обработване и да не могат да се променят. Фактът, че обработването на лични данни е ограничено, следва да бъде ясно посочен в системата.

Чл.58. (1) Действията по осъществяване на киберсигурност, във връзка със защитата на лични данни, се прилагат от системния администратор на Областна администрация Варна в съответствие с Вътрешните правила за мрежова и информационна сигурност.

(2) При сключване на договор с доставчик на софтуерен продукт, относим или директно приложим в администрирането на лични данни, отговорностите на доставчика се уреждат с договор между него и администратора на лични данни в лицето на областния управител на област Варна.

(3) Доставчикът на продукта за администриране на лични данни на физически лица или водене на регистри, свързани с тази дейност, носи отговорност за съвместимостта на предложения продукт с изискванията на приложимото законодателство и адекватните мерки за защита на информацията.

(4) В случай на санкция, наложена на администратора на лични данни по вина на доставчика на специализирания софтуерен продукт, доставчикът следва да поеме имуществената отговорност по погасяване на задължението.

(5) В случай, че администраторът използва електронни регистри за дейностите по защита и обработка на личните данни, които запазват информацията на външен за ведомството сървър, потребителят администратор следва при прекратяване на абонамента да получи от доставчика цялата въведена информация в машинно четим формат.

САНКЦИИ

Чл.59. (1) Всяко лице, което е претърпяло материални или нематериални вреди в резултат на нарушение на нормативните разпоредби, има право да получи обезщетение от администратора или обработващия лични данни.

(2) Администраторът, участващ в обработването на лични данни, носи отговорност за вреди, произтичащи от извършеното обработване, което нарушава установените правила. Тази отговорност възниква само когато администраторът не е изпълнил свои задължения по

имуществената санкция не може да надвишава сумата, определена за най-тежкото нарушение.

ДОПЪЛНИТЕЛНИ РАЗПОРЕДБИ

§1. Настоящите Вътрешни правила за обработване и защита на личните данни на физически лица в Областна администрация Варна влизат в сила от датата на утвърждаването им със заповед на областния управител и отменят всички предходни инструкции със същия предмет във ведомството.

§2. В случаите, когато със специален закон или подзаконов нормативен акт е предвиден особен ред за работа с лични данни на физически лица, различен от установения по-горе, настоящите правила не се прилагат.

§3. Преди да бъдат утвърдени от областния управител, Вътрешните правила за обработване и защита на личните данни на физически лица се съгласуват от главния секретар на ведомството, на който се възлага и контрола по изпълнението им.

§4. Областният управител назначава или сключва договор с лице по защита на личните данни, което е подчинено единствено на него.

§5. Административният орган не е длъжен да изпълни неоснователно, незаконосъобразно или явно прекомерно искане на субект на данни, или такова, което съдържа очевидно противоречие с нормативно установено задължение на администратора.

§6. Неразделна част от настоящите Вътрешни правила за обработване и защита на личните данни на физически лица в Областна администрация Варна са три приложения: два образеца на декларации - една за информирано съгласие от физическо лице, когато не е налице правно основание или задължение за обработване на негови лични данни и една за поверителност; регистър за информираност на служителите относно правилата за работа с лични данни на физически лица.